

The Entropy Region is not Closed Under Duality

Tarik Kaced

email: tarik.kaced@ens-lyon.org

Abstract—We import a duality notion coming from polymatroids to define duality for information inequalities. We show that the entropy region for $n \geq 5$ is not closed under duality. Our result answers an open question of Matúš [13] (1992).

I. INTRODUCTION

Let $(X_i)_{i \in N}$ be n discrete random variables. To each non-empty subset of variables $X_J = \{X_i : i \in J \subseteq N\}$, we can associate the Shannon entropy $H(X_J)$. The *entropic vector* $(H(X_J))_{\emptyset \neq J \subseteq N}$ is a point in the $2^n - 1$ -dimensional Euclidean space $\mathbb{R}^{2^n - 1}$. We denote by $\mathbf{H}_N^{\text{ent}}$ the set of all entropic points. $\mathbf{H}_N^{\text{ent}}$ is a solid object, but not closed in general [16]. The closure of $\mathbf{H}_N^{\text{ent}}$ is what we call the entropy region, it is the set of $2^n - 1$ -dimensional real vectors that are limits of entropic vectors. In fact, $\text{cl}(\mathbf{H}_N^{\text{ent}})$ is a convex cone whose boundary can be delimited by hyperplanes. Such a hyperplane defines a linear inequality of entropy terms: an information inequality. Information inequalities live in the dual¹ cone $(\mathbf{H}_N^{\text{ent}})^* = \{c \in \mathbb{R}^{2^n - 1} : \langle c, h \rangle \geq 0, h \in \mathbf{H}_N^{\text{ent}}\}$. A point $c = (c_J)_{\emptyset \neq J \subseteq N}$ in the dual cone $(\mathbf{H}_N^{\text{ent}})^*$ commonly corresponds to the coefficients of a linear information inequality, often rewritten as

$$\sum_J c_J H(X_J) \geq 0.$$

Characterizing the entropy region using information inequalities is no easy task, a full description is already lacking when $n \geq 4$ for it is not polyhedral [11].

Fujishige noticed that entropic vectors are in fact polymatroids [5] in the following sense. A polymatroid is a real-valued function f defined on subsets of the ground set N that is non-negative, non-decreasing, and submodular:

$$\forall A, B \subseteq N, f(A) + f(B) \geq f(A \cup B) + f(A \cap B).$$

Indeed, submodularity is related to Shannon's basic inequality:

$$H(A, C) + H(B, C) \geq H(A, B, C) + H(C),$$

It states that the conditional mutual information $I(A:B|C)$ is non-negative. The set of positive linear combinations of instances of the basic inequality are called the *Shannon-type* inequalities.

¹This duality notion is not the polymatroid duality notion we are looking for.

The duality notion we allude to in the title of this paper comes from polymatroid theory. Common operations on the set of polymatroids include direct sums, linear combinations, minors: deletion and contraction, convolutions, and duals. Apart from the last one, all other operations have entropic counterparts. We thus concentrate on the under-examined notion of polymatroid duality. Let f be a polymatroid on N , define the function

$$f^\perp(J) = f(N \setminus J) - f(N) + \sum_{j \in J} f(j).$$

Then f^\perp is again a polymatroid on N and is called the dual polymatroid. This operation immediately begs for a similar question for almost entropic vectors: the elements of $\text{cl}(\mathbf{H}_N^{\text{ent}})$.

Question 1. *Is the dual of an almost entropic polymatroid still almost entropic?*

This question is related to open problems about polymatroid duality that can be found in [13]. To attack this question, we propose to shift the point-of-view to information inequalities. The key idea is to import the notion of polymatroid duality into information inequalities and reformulate Question 1 in this setting. Our main theorem provides a negative answer to Question 1 as a corollary.

Theorem 1 (Main Theorem). *The entropy region is not closed under duality for $n \geq 5$*

In the rest of this paper, we provide some properties of our duality notion and its connection with balanced inequalities. We study its meaning for different kinds of information inequalities.

II. PRELIMINARIES AND PROPERTIES

For the sake of conciseness we make the following use of notations. We usually omit commas in entropic terms and by $H(AB)$ we mean $H(A, B)$. An instance of an inequality \mathcal{I} is simply a version of \mathcal{I} for some variables assignment. A conditional version of an inequality \mathcal{I} is a version of \mathcal{I} wherein each entropy term $H(X_J)$ has been replaced by $H(X_J|Z)$, where Z is a fresh random variable. If \mathcal{I} is valid, then so is its conditional version. We denote the conditional Ingleton inequality quantity

in the following way:

$$\text{Ingl}(A:B, C:D|E) = I(A:B|CE) + I(A:B|DE) + I(C:D|E) - I(A:B|E).$$

The famous Ingleton inequality [7] thus rewrites as $\text{Ingl}(A:B, C:D|\emptyset) \geq 0$.

A. Duality and balancing

Definition 1 (Balanced Inequalities). *An n -variable information inequality $c \in (\mathbf{H}_N^{\text{ent}})^*$ is balanced if the sum of the coefficients involving X_i is zero, for each $i \in N$*

$$\forall i \in N, \sum_{i \in J \subseteq N} c_J = 0.$$

Given a valid linear information inequality, its balanced counterpart is also valid [1].

Proposition 1 (Balanced Inequalities, Chan [1]). *Let $(c_J)_{J \subseteq N}$ be a list of coefficients, the following are equivalent:*

- The inequality

$$\sum_{J \subseteq N} c_J H(X_J) \geq 0 \quad (1)$$

is a valid information inequality.

- The inequality

$$\sum_{J \subseteq N} c_J H(X_J) - \sum_{j \in N} r_j H(X_j | X_{N-j}) \geq 0, \quad (2)$$

where r_j is the sum of all c_J involving X_j , is a valid balanced information inequality.

We say that (2) is the balanced version of (1).

We introduce a dual operator for information quantities.

Definition 2 (Dual operator). *Let n be a number of variables, the dual operator $^\perp$ is defined as an operator that maps any entropic quantity to a dual quantity by replacing entropy terms as follows:*

$$H^\perp(X_J) \stackrel{\text{def}}{=} -H(X_J | X_{N \setminus J}) + \sum_{j \in J} H(X_j). \quad (3)$$

We are now able to define the formal dual of an information inequality by defining its dual coefficients.

Definition 3 (Dual coefficients). *Let $c = (c_J)_{\emptyset \neq J \subseteq N}$ be the coefficients of an inequality. We define the formal dual inequality c^\perp as the coefficients of the dual of c :*

$$\left[\sum_J c_J H(X_J) \right]^\perp = \sum_J c_J H^\perp(X_J) \stackrel{\text{def}}{=} \sum_J c_J^\perp H(X_J)$$

Definition 4 (Self-dual inequality). *We say that an inequality c is self-dual if c^\perp is an instance of c or a conditional version of c .*

We are now able to prove some properties of this duality notion. Let us show it behaves as a dual, modulo balancing².

Proposition 2. *Let $c \in (\mathbf{H}_N^{\text{ent}})^*$ be an information inequality, then:*

- 1) c^\perp is balanced,
- 2) if c is balanced, then $c^{\perp\perp} = c$,
- 3) if c is not balanced, then $c^{\perp\perp}$ is the balanced version of c .

Proof: Let $c \in (\mathbf{H}_N^{\text{ent}})^*$ be an inequality and c^\perp its formal dual. Let $i \in N$ be a variable index and $J \subseteq N$.

1. We compute the contribution of each term $c_J H^\perp(X_J)$ to the sum r_i of coefficients involving X_i . We have

$$c_J H^\perp(X_J) = c_J [H(X_{N \setminus J}) - H(X_N) + \sum_{i \in J} H(X_i)],$$

if $i \in J$, then the contribution of $c_J H^\perp(X_J)$ is

$$c_J [0 - 1 + 1] = 0,$$

if $i \notin J$, then the contribution of $c_J H^\perp(X_J)$ is

$$c_J [1 - 1 + 0] = 0.$$

Overall, for any i , $r_i = 0$, which implies c is balanced.

2. We compute the contributions of each term $c_J H(X_J)$

$$[c_J H(X_J)]^{\perp\perp} = c_J [H^\perp(X_{N \setminus J}) - H^\perp(X_N) + \sum_{i \in J} H^\perp(X_i)]$$

$$H^\perp(X_{N \setminus J}) = H(X_J) - H(X_N) + \sum_{i \in J} H(X_i)$$

$$H^\perp(X_N) = -H(X_N) + \sum_{i \in N} H(X_i)$$

$$H^\perp(X_i) = -H(X_i | X_{N \setminus \{i\}}) + H(X_i)$$

By collecting every term we get after cancelling:

$$\sum_{J \subseteq N} c_J H(X_J) - \sum_{i \in N} r_i H(X_i | X_{N-i}),$$

where r_i is the sum of all c_J involving X_j . That is we get the balanced version of the original inequality c .

3. The first two properties imply the third one. \blacksquare

Remark 1. *The duality notion from [10] is an involution on the set of polymatroids and induces a involution on all information inequalities which coincides with ours on balanced information inequalities. Although it would get rid of the need of balanced inequalities, their notion is made slightly more complex by additional terms to artificially ensure that the "private information" of a polymatroid is not lost.*

²Properties "modulo balancing" were first spotted in [8].

B. Polymatroid and vector spaces

The polymatroid region \mathbf{H}_N is the closure of the set of all polymatroids on the ground set N of size n . It is the polyhedral cone delimited by Shannon-type inequalities. It is an outer bound of the entropy region. The following well-known proposition implies that the dual of a polymatroid is again a polymatroid. Our proof highlights how duality works on basic inequalities.

Proposition 3. *The polymatroid region is closed under duality for any $n \geq 0$*

Proof: It suffices to show that the dual of Shannon's basic inequality is valid.

$$\begin{aligned} [I(A:B|C)]^\perp &= H^\perp(AC) + H^\perp(BC) - H^\perp(ABC) - H^\perp(C) \\ &= -H(AC|BD) + H(A) + H(C) - \\ &\quad -H(BC|AD) + H(B) + H(C) + \\ &\quad +H(ABC|D) - H(A) - H(B) - H(C) + \\ &\quad +H(C|ABD) - H(C) \\ &= H(BD) + H(AD) - H(C) - H(ABD) \\ [I(A:B|C)]^\perp &= I(A:B|D) \geq 0 \end{aligned}$$

We have just proved that Shannon's basic inequality, $I(A:B|C) \geq 0$, is self-dual, which implies the result. ■

An interesting subset of entropic vectors is the one arising from vector subspaces. Let V be a vector space over \mathbb{F}_q and $V_1, V_2, \dots, V_n \subseteq V$ be n vector subspaces. Denote by V_J the sum vector subspace $\langle \{V_i, i \in J\} \rangle$, then the point $(\log q \cdot \dim(V_J))_J$ is an entropic vector [6]. The closure of the set of all such points is called the Ingleton region $\mathbf{H}_N^{\text{Ingl}}$.

Proposition 4. *The Ingleton region is closed under duality for $n \geq 0$*

This result is a corollary of the construction of a representation of the dual polymatroid. A proof of the dual representation can be found in [15], it is based on a matroidal version from Oxley's Matroid Theory book for matroids [14]. Such a construction based on vector space orthogonality has been used in several constructions related to information theory (see [3], [4]). In our case, Proposition 4 follows from the fact that the dual of an entropic point arising from vector subspaces is also an entropic point coming from vector subspaces and Proposition 2.

Duality induces symmetries that were somehow missed. For instance, notice that Ingleton inequality is self-dual:

Lemma 1. *On variables A, B, C, D, E, F , we have:*

$$\text{Ingl}^\perp(A:B, C:D|E) = \text{Ingl}(C:D, A:B|F).$$

Proof: The theorem statement is the most general but for simplicity we prove the unconditional version on 4 variables: $\text{Ingl}^\perp(A:B, C:D) = \text{Ingl}(C:D, A:B)$. The

more general results follows from the same type of computations.

$$\begin{aligned} &[I(A:B|C) + I(A:B|D) + I(C:D) - I(A:B)]^\perp \\ &= I(A:B|D) + I(A:B|C) + I(C:D|AB) - I(A:B|CD) \\ &= I(C:D|A) + I(C:D|B) + I(A:B) - I(C:D) \end{aligned}$$

In the first equation, the dual operator applies linearly, therefore Proposition 3 can be applied. The last equation is gotten by rearranging the entropy terms. ■

The inequalities on the ranks of five vector subspaces have been studied by Dougherty *et al* [2]. They found 24 new rank inequalities on five variables. If we account for duality, the list of 24 inequalities reduces to 13, as some inequalities are dual of one another or self-dual.

III. MAIN RESULT

Lemma 2 (MMRV inequality [9]). *The following is a non-Shannon-type information inequality.*

$$I(A:B) \leq I(A:B|C) + I(A:B|D) + I(C:D) + I(A:B|E) + I(A:E|B) + I(B:E|A) \quad (4)$$

We are now ready to prove the main theorem.

Proof of Theorem 1: We prove that the formal dual of the MMRV inequality on five variables is not a valid information inequality. We provide a counter-example by exhibiting a binary joint distribution for variables A, B, C, D, E .

Let us first compute the formal dual of inequality (4). We first make appear the Ingleton quantity.

$$[\text{Ingl}(A:B, C:D) + I(A:B|E) + I(A:E|B) + I(B:E|A)]^\perp$$

The dual operator acts linearly, so we take the dual of each term and obtain the following quantity:

$$\text{Ingl}(C:D, A:B|E) + I(A:B|CD) + I(A:E|CD) + I(B:E|CD)$$

which rewrites after expanding the Ingleton term as:

$$\begin{aligned} &I(C:D|AE) + I(C:D|BE) + I(A:B|E) - I(C:D|E) + \\ &+ I(A:B|CD) + I(A:E|CD) + I(B:E|CD). \end{aligned}$$

We show that the previous quantity can be negative and thus cannot induce a valid information inequality. Consider the distribution on A, B, C, D, E induced by the following tuples with positive probability masses as shown.

A	B	C	D	E	Prob
0	0	0	0	0	ϵ
0	0	0	0	1	$1/4 - \epsilon$
0	1	0	0	1	$1/4 - \epsilon$
0	1	1	0	0	ϵ
1	0	0	0	1	$1/4 - \epsilon$
1	0	0	1	0	ϵ
1	1	0	0	0	ϵ
1	1	0	0	1	$1/4 - \epsilon$

For this particular distribution on (A, B, C, D, E) , all terms of the dual quantity are zeroes except for two. $I(C:D|AE) = 0$ since given any value of (A, E) , either C or D is deterministic. A similar argument shows $I(C:D|BE) = 0$. Given each value of E , the tuple (A, B) is uniformly distributed among all possible values, thus $I(A:B|E) = 0$. To check that $I(A:E|CD) = 0$, we see that given some value of (C, D) either (A, E) is deterministic or the distributions of A and E are independent (when $(C, D) = (0, 0)$). The case of $I(B:E|CD)$ is similar. For the positive terms, we rely on formal computations which give:

$$\begin{aligned} I(C:D|E) &= \Theta(\varepsilon), \\ I(A:B|CD) &= \Theta(\varepsilon^2). \end{aligned}$$

Therefore the formal dual inequality cannot hold for small values of ε . ■

We answer an open question of Matúš [13].

Corollary 1. *The dual of an almost representable matroid is not necessarily almost representable.*

Proof: According to the main theorem, the entropy region is not closed under duality. It implies there exist an entropic polymatroid v whose dual is not almost entropic. By [12, Theorem 5], there exist a sequence of entropic matroids that can asymptotically factor into a multiple of v (by grouping elements). Thus one of these entropic matroids must have a non-representable dual.

Notice that this proof is not constructive, however it can be made so by using the explicit entropic polymatroid from the main theorem. Let us call it v , its dual polymatroid v^\perp does not satisfy the MMRV inequality. Thus we can construct an entropic matroid whose dual is not entropic in the following way. Approximate v by a (close enough) rational entropic vectors; use free expansion to expand an integer multiple of v into an entropic matroid m . In this way, m is entropic but m^\perp is not almost entropic: it fails the MMRV inequality. ■

The previous proof provides a construction for an entropic matroid whose dual is not almost entropic, however no minimality claim is made. The smallest entropic matroid whose dual is not almost entropic is not known.

IV. DISCUSSION

This new geometrical property of the entropic region depicts a bigger geometric picture. The entropic region is a cone that is not stable by duality and that is stuck between two cones: the inner bound $\mathbf{H}_N^{\text{Ingl}}$ and the outer bound \mathbf{H}_N that are both stable by duality. The case of duality of the entropy region for $n = 4$ is still open.

In future work, we investigate the case of information inequalities duality in other settings, especially in quantum information inequalities [10]. This notion of duality seems very general, in fact it applies to any concept

expressible via entropy. It can reveal dualities between information theoretic problem, for instance the secret-sharing problem is self-dual in the following sense. Any secret-sharing instance expressed with entropy maps to another secret-sharing instance under the dual operator. In fact the dual instance is the secret-sharing problem for the dual access structure. In general, we expect a class of problems to be the dual of a different class of problems.

REFERENCES

- [1] T. H. Chan. Balanced information inequalities. *IEEE Trans. Inf. Theor.*, 49(12):3261–3267, December 2003.
- [2] Randall Dougherty, Christopher F. Freiling, and Kenneth Zeger. Linear rank inequalities on five or more variables. *CoRR*, abs/0910.0284, 2009.
- [3] Oriol Farràs, Torben Brandt Hansen, Tarik Kaced, and Carles Padró. On the information ratio of non-perfect secret sharing schemes. *Cryptology ePrint Archive*, Report 2014/124, 2014. <http://eprint.iacr.org/2014/124>.
- [4] Serge Fehr. Efficient construction of the dual span program. Manuscript, 1999.
- [5] Satoru Fujishige. Polymatroidal dependence structure of a set of random variables. *Information and Control*, 39(1):55 – 72, 1978.
- [6] Daniel Hammer, Andrei Romashchenko, Alexander Shen, and Nikolai Vereshchagin. Inequalities for Shannon Entropy and Kolmogorov Complexity. *J. Comput. System Sci.*, 60(2):442–464, 2000.
- [7] A. W. Ingleton. Representation of matroids. *Combinatorial Mathematics and its Applications*, 1971.
- [8] T. Kaced. Equivalence of two proof techniques for non-shannon-type inequalities. In *Information Theory Proceedings (ISIT)*, 2013 *IEEE International Symposium on*, pages 236–240, July 2013.
- [9] K. Makarychev, Y. Makarychev, A. Romashchenko, and N. Vereshchagin. A new class of non-shannon-type inequalities for entropies. *Communications in Information and Systems*, 2(2):147–166, 2002.
- [10] František Matúš. Polymatroids and polyquantoids. *CoRR*, abs/1210.7931, 2012.
- [11] František Matúš. Infinitely many Information Inequalities. *Proceedings ISIT 2007*, pages 41–44, 2007.
- [12] František Matúš. Two constructions on limits of entropy functions. *IEEE Trans. Inf. Theor.*, 53(1):320–330, January 2007.
- [13] František Matúš. Ascending and descending conditional independence relations, 1992.
- [14] J. G. Oxley. *Matroid Theory*. Oxford University Press, New York, 1992.
- [15] Carles Padró. Lecture notes in secret sharing. *Cryptology ePrint Archive*, Report 2012/674, 2012. <http://eprint.iacr.org/>.
- [16] Zhen Zhang and Raymond W. Yeung. A non-Shannon-type Conditional Information Inequality. *IEEE Trans. on Inform. Theory*, 43:1982–1986, 1997.